AO 93 (Rev. 12/03) Search Warrant

UNITED STATES DISTRICT COURT

Western District of North Carolina

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

Google Legal Investigations Support
1600 Amphitheatre Parkway
Mountain View, California 94043

SEARCH WARRANT

Case Number: 1:10mj3

TO: Derek Farmer and any Authorized Officer of the United States

Affidavit(s) having been made before me by Derek Farmer (Affiant) who has reason to believe

that ☐ on the person of, or ☑ on the premises known as (name, description and/or location)

1600 Amphitheatre Parkway
Mountain View, California 94043

in the Northern District of California there is now concealed a certain person or property, namely (describe the person or property)

see Attachment B

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before Feby 1, 2010 (Date)

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search ☑ in the daytime — 6:00 AM to 10:00 P.M. ☐ at anytime in the day or night as I find reasonable cause has been established and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Dennis L. Howell as required by law.

U.S. Magistrate Judge (Rule 41(f)(4))

Jany 22, 2010 at 5:52 pm (Date and Time Issued) at Asheville, North Carolina (City and State)

Dennis L. Howell
Name and Title of Judge
United States Magistrate Judge

Dennis L. Howell
Signature of Judge

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Gmail (Google)

To the extent that the information described in this attachment is within the possession, custody, or control of Gmail (Google), Gmail (Google) is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

e. All records and content pertaining to communications through the Google Talk "lilninjaskills" user account and any person, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations 18 U.S.C. § 2251(a) and 18 U.S.C. § 2252, and any statutes listed on the application for a search warrant or search warrant involving Paul Lawrence Berrell for each account, identifier, or user ID identified listed on Attachment A.

UNITED STATES DISTRICT COURT

Western DISTRICT OF North Carolina

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

Google Legal Investigations Support
1600 Amphitheatre Parkway
Mountain View, California 94043

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number: 1:10mj3

I, Derek Farmer being duly sworn depose and say:

I am a(n) FBI Special Agent and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)

1600 Amphitheatre Parkway
Mountain View, California 94043

in the Northern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

see attachment B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

see attached affidavit

concerning a violation of Title 18 United States code, Section(s) 2251(a), 2252

The facts to support a finding of probable cause are as follows:

see attached affidavit

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

Aug 23, 2010 at Asheville NC
Date City State

Dennis L. Howell Magistrate Judge
Name of Judige Title of Judge

Signature of Judge

E-MAIL ACCOUNT SEARCH WARRANT AFFIDAVIT

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH LILNINJASKILLS@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GMAIL (GOOGLE)	Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Derek Farmer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Gmail (Google), an e-mail provider headquartered at Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since February 1, 2009. I am currently assigned to the Charlotte Field Office Cyber squad

within the FBI and conduct investigations involving the online sexual exploitation of children. I have most recently received technical training in Linux for Law Enforcement Officers (LEOs) and Internet Investigations. Additionally, I have received certifications in Computer Technology Industry Association (CompTIA) A+ and CompTIA Network+. CompTIA A+ certification is the industry standard for computer support technicians, while CompTIA Network+ certifies network professionals, per CompTIA.

3. I was employed previously in the Information Technology Advisory practice with KPMG LLP. While employed with KPMG LLP, I assessed clients current state of information security in context of their enterprise wide systems. I also assisted clientele in designing and implementing appropriate measures to protect information assets. Additionally, I helped to ensure that appropriate security controls were in place for protection of an organization's key information assets. Lastly, I helped clients reduce the risk of critical services being disrupted by availability, disasters or interruptions.

4. I was also employed by the United States Army. While employed with the United States Army, I resolved installation level problems in personnel databases and accounted for over $250,000 worth of computer equipment. I also supervised preventive maintenance and repairs to installation servers. I also provided help desk customer support for technical problems and questions. I also used technical training, experience, and common sense to make corrective actions and resolve automation problems.

5. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from Asheville, North Carolina Police Department Detective Tony Johnson, other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

TECHNICAL BACKGROUND

7. In general, an email that is sent to a Gmail (Google) subscriber is stored in the subscriber's "mail box" on Gmail (Google) servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Gmail (Google) servers indefinitely.

8. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Gmail (Google) servers, and then transmitted to its end destination. Gmail (Google) often saves a copy of the sent email. Unless the sender of the email specifically deletes the email from the Gmail (Google) Inc. server, the email can remain on the system indefinitely.

9. A Gmail (Google) subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Gmail (Google).

10. Subscribers to Gmail (Google) might not store on their home computers copies of the emails stored in the Gmail (Google) account. This is particularly true when they access their

Gmail (Google) account through the web, or if they do not wish to maintain particular emails or files in their residence.

11. In general, email providers like Gmail (Google) ask each of their subscribers to provide certain personal identifying information when registered for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

12. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Gmail [Google] website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

13. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user as a result of the communication.

14. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

PROBABLE CAUSE

15. On May 18, 2009, a concerned mother reported to the Asheville Police Department that she suspected her minor daughter of having an inappropriate relationship with an adult male. The victim's mother had found information on her daughter's computer, including a photograph, which caused her to be suspicious. The photograph depicted her daughter in an embrace with the suspect, Paul Lawrence Berrell; both the minor and Berrell had their shirts off. At the time, Berrell was the minor victim's music teacher at the Asheville Catholic School, and was also the music minister at the St. Eugene's Catholic Church.

16. Interviews conducted by Asheville Police Criminal Investigations Detective Sergeant David Romick and Detective Mandy Buchanan of both the minor victim and the suspect, Paul Lawrence Berrell, showed that an inappropriate relationship had existed between the two. After being shown the previously-mentioned photo, Berrell admitted to transporting the minor victim to his apartment (without the victim's parent's approval) in May of 2009. Berrell stated that the victim had wanted to see a surgical scar on his chest, so he took off his shirt. Berrell stated that the victim took off her shirt, too, on her own accord, and the photo was taken.

Berrell stated that he never engaged in sexual activity with the victim. This was later found to be a false statement.

17. Berrell gave verbal consent for Detective Buchanan and Sergeant Romick to seize a desktop computer located in his residence, and for a trained examiner to search it.

18. Based on Berrell's verbal consent to search, Sergeant Romick and Detective Buchanan seized a Hewlett Packard (HP) Pavilion computer, Serial Number (SN): MXF60200V4 from Berrell's residence and placed it into the care and custody of the Asheville Police Property Section. Also, on the same date, the victim's mother brought in the victim's Compaq Presario laptop computer, SN: F762NR and turned it over to detectives Romick and Buchanan for analysis.

19. On May 19, 2009, Detective Tony Johnson, a computer forensic examiner with the Asheville Police Departement, was notified that Sergeant Romick and Detective Buchanan had seized a HP Pavilion computer, SN: MXF60200V4, and that a forensic analysis of the machine was needed.

20. On May 19, 2009, Detective Johnson coordinated with the Asheville Police Property Section manager, Lee Smith, to check out the HP Pavilion computer from the Property Section, in order to facilitate the forensic analysis of the machine. Following standard operating procedures, Detective Johnson forensically acquired a copy of the HP Pavilion's hard drive and began analysis of the data.

21. On May 21, 2009, Detective Johnson located a movie file that contained child pornography, while analyzing the data on the HP Pavilion's hard drive. Detective Johnson knew

the movie file depicted child pornography based on his knowledge, training and experience. The movie file had the following file name, as identified on the hard drive: Ls-Magazine Lsm 09-04-02 pthc.young lolitas ((lolitaguy))((hussyfan)).avi. The movie file was six minutes and eight seconds long (6:08), and it depicted two white female minors, approximately 10 to 12 years of age, naked together on a bed. Throughout the length of the movie, the children are shown lasciviously displaying their genitals to the camera, masturbating, touching and licking each other's inner thighs and vaginal areas. Detective Johnson ceased the analysis of the data in order to document and report the contraband movie file. Detective Johnson then obtained a search warrant to continue the analysis.

22. Detective Johnson drafted and presented a search warrant on May 21, 2009, which was accepted by Senior Magistrate Kdan. Detective Johnson served the search warrant on May 21, 2009, and continued the analysis of the Berrell data.

23. At the conclusion of the analysis, Detective Johnson presented evidence to the United States Attorney's Office (USAO), which showed that Berrell did have a sexual relationship with the victim. On Berrell's hard drive, Detective Johnson located graphic pictures depicting the victim in various states of undress and performing a sexual act with Berrell. In addition, Detective Johnson obtained evidence of online communications between Berrell and the victim, using Google Talk (a chat program) with screen names, "bigninjaskills" and "LilNinjaSkills", in which Berrell and the victim discuss oral sex.

24. Detective Johnson also located further evidence of child exploitation (contraband movies and images) on the HP Pavilion's hard drive. Specifically, forty movies and one hundred forty-one images contained images related to child exploitation. Detective Johnson noted one

file named, "(yamad)Little Boy Bondage 11Yo and Men Full Version – Gay Pedo Ptch.mpg". This specific file was a movie file, nineteen minutes and fourteen seconds long (19:04), and it depicts a white male minor, approximately 9 to 11 years of age. At various points throughout the movie, the child was shown bound in various sadomasochistic manners (his arms bound behind his back and tethered to a rope around his neck). Two adult males make the boy perform oral sex on them and also anally penetrate the child. The men flog the child with a leather belt and physically assault him. Detective Johnson also noted one instance of an image file containing evidence of child exploitation. The file was named, "JPEG_25618956[536650].jpg", and it depicts a white female minor, approximately 10 to 12 years of age, performing oral sex on a white male. Detective Johnson submitted these child pornography videos and pictures to the National Center for Missing and Exploited Children (NCMEC) for analysis. According to NCMEC, the two files mentioned in this paragraph, along with numerous other files, contained known victims of child pornography and sexual exploitation. This child exploitation video was located in the recycle bin of Berrell's computer but forensic investigation revealed that it had been placed there by a third party just prior to seizure by the police. It had not been successfully permanently deleted.

25. The victim's mother reported finding evidence on her daughter's laptop computer, Compaq Presario, Serial Number (SN): F762NR, which she suspected was chats between the victim and Berrell. The victim's mother stated that Berrell used the screen name "bigninjaskills" and the victim used "LilNinjaSkills".

26. As previously mentioned, the victim's mother gave Detective Buchanan and Sgt. Romick a Compaq Presario laptop computer (SN F762NR) identified as having belonged to the

victim. Consent to search the victim's laptop was also given by the victim's mother. Detective Johnson began an analysis of the victim hard drive on May 30, 2009. During the forensic analysis of the victim's hard drive, Detective Johnson used a search function built into the forensic software to search for references to "bigninjaskills". Detective Johnson located two document files containing saved chats between the victim and Berrell using "bigninjaskills" and "LilNinjaSkills".

27. Detective Johnson also found evidence on the Berrell's hard drive using bigninjaskills@gmail.com to send text messages to the victim's cellular telephone.

28. It is my belief that there is probable cause to believe that further evidence of Berrell's illegal sexual relationship with the victim and child exploitation activities may exist in information associated with lilninjaskills@gmail.com that is stored at premises controlled by Gmail (Google). Based on the facts presented, and the affiant's training and experience, the affiant believes that probable cause exists to search the information associated with lilninjaskills@gmail.com that is stored at premises controlled by Gmail (Google) for evidence of the previously mentioned criminal activity.

CONCLUSION

29. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Google there exists evidence of a crime and contraband or fruits of a crime. Accordingly, a search warrant is requested.

30. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. § 2703(a).

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

32. In consideration of the foregoing, I respectfully request that this court issue a search warrant to further search the items listed and described in Attachment B.

Respectfully submitted,

Derek S. Farmer
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 22, 2010:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with lilninjaskills@gmail.com that is stored at premises owned, maintained, controlled, or operated by Gmail (Google), a company headquartered at Google Legal Investigations Support, 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Gmail (Google)

To the extent that the information described in this attachment is within the possession, custody, or control of Gmail (Google), Gmail (Google) is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

e. All records and content pertaining to communications through the Google Talk "lilninjaskills" user account and any person, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations 18 U.S.C. § 2251(a) and 18 U.S.C. § 2252, and any statutes listed on the application for a search warrant or search warrant involving Paul Lawrence Berrell for each account, identifier, or user ID identified listed on Attachment A.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature